U.S. Department of Energy Headquarters
Office of the
Chief Information Officer

Cyber Security Program Plan

For

The Headquarters Site

November 2000

Office of the Chief Information Officer
Office of the Associate Chief Information Officer for Operations
Division of Network, Telecommunications and Engineering

Executive Summary

This Cyber Security Program Plan (CSPP) has been developed as directed by the Department of Energy Unclassified Cyber Security Program Notice (DOE Notice 205.1). The role of the Office of the Associate CIO for Operations (OCIO/OPS) is in managing, maintaining and securing the DOE HQ site operations. Individual DOE HQ Secretarial Offices are responsible for managing and maintaining their LANs following policy and procedures provided in this CSPP.

The federal information processed on the DOE HQ site, including the information processed on the Secretarial Office Local Area Networks (LANs), is sensitive and requires protection measures commensurate with the value of the information and infrastructure as determined by the appropriate risk assessment.

Because of the interconnectivity of the DOE HQ Secretarial Office LANs (e.g., DP, SC, EE, FE, etc.), security failures could jeopardize other networks as well as the information processed on other individual DOE HQ Secretarial Office LANs. This CSPP describes the HQ site and the interoperability between Secretarial Office LANs, and the policies and procedures that have been implemented to ensure the integrity, availability, and confidentiality of these important and valuable information processing and data resources.

This DOE HQ site CSPP, in concert with the Unclassified Computer Security Program, DOE Notice 205.1, establishes the basic guideline and direction for use by all DOE HQ Secretarial Offices. Each Secretarial Office is to develop and apply a comprehensive organizational CSPP, applicable application CSPPs, and have implemented appropriate security measures.

Introduction

Purpose

The purpose of this CSPP document is to convey the security controls/policies to be employed within the OCIO, and all directly attached Secretarial Office LANs. It also serves to increase awareness of all DOE HQ network support employees on the importance of maintaining appropriate information security policies, procedures and standards. This awareness applied to the DOE HQ Network environment, and the roles in maintaining compliance with technical procedures is essential to continued operational integrity of the DOE HQ networking operations. (Note: The HQ site Network Information Security Policy and Technical Security Policies and Procedures [TSPP] documents the detailed technical procedures used to implement security by the OCIO within the HQ site. This document is referenced extensively within this CSPP). The awareness of security policy applies to the overall integrity of the DOE HQ site operations throughout the DOE HQ networked computing environment. The CSPP also assigns specific responsibilities for the protection of data and information, and for the information security of the DOE HQ site and directly attached Secretarial Office LAN resources.

Scope

All information assets and services processed automatically or manually, and utilized by the HQ site networking operations, are covered by this CSPP. The CSPP applies equally to all servers attached within the HQ site LANs and any peripheral network devices such as routers and switches, workstations, and personal computers within the DOE HQ computing environment. The CSPP also applies to network computing and communications resources including data, information, software, hardware, facilities, telecommunications resources, and information security monitoring systems and safeguards.

The policies defined herein are applicable to all DOE HQ employees and authorized contractors who are associated with the site network operations. The policies may also be applicable to any authorized contractors where network-computing resources have connectivity with the DOE HQ site.

Explicit definitions of interconnectivity for systems and services (e.g., LANs, intrusion detection systems, Firewall systems, Virtual Private Networks, major applications, etc.) that are under the authority of other DOE HQ Secretarial Offices are within the scope of this document. This DOE HQ site CSPP, in concert with the Unclassified Computer Security Program, DOE Notice 205.1, establishes the basic guideline and direction for use by all DOE HQ Secretarial Offices. Each is to develop and apply a comprehensive organizational CSPP for their systems and have implemented appropriate security measures. While this CSPP is primarily directed toward HQ prerogatives, the format and contents contained herein are applicable to the DOE Secretarial Offices and are to be used to develop other CSPP documents.

VI. Cyber Security Controls and Policies

L. Headquarters (HQ) Site Policies

4. Virus Protection Policy

Policy

The Office of the Chief Information Officer (CIO), as the central cyber security authority for the Headquarters site, will utilize the following cyber security policies pertaining to virus, worm, Trojan horse, and other malware protection for the Headquarters network:

- All workstations, portable computers, servers and applicable network devices (including but not limited to network servers, database servers, Web servers, e-mail servers/post offices, e-mail gateways, and firewalls) must have anti-viral protection software installed and activated, *where possible*. An anti-virus monitoring (memory-resident) program must be initiated on all systems during boot-up and remain active during usage. The anti-viral software used must be current and updated on all systems as new versions and signature files become available (at least weekly).

- Where content checking is available (such as for e-mail post offices), that feature must be used to detect and block virus transmission of e-mail or files that meet known threat criteria and can be intercepted through content identification (such as standard subject lines or file types). Content checkers should also be used to identify and quarantine known hoax messages.

- All malware detected by anti-virus software on any media or computing device within DOE Headquarters must be reported to the Headquarters Automated Systems Security Incident Support Team (ASSIST) via the Infrastructure Support Center (Help Desk) at 301-903-2500 (response number 2). This ensures that proper containment and eradication is performed and that other endangered parties are identified and alerted.

Scope

This policy affects all organizations operating on the Headquarters site network.

Roles and Responsibilities

The Associate CIO for Operations has established the DOE Headquarters Automated Systems Security Incident Support Team (ASSIST), which acts as the coordinator for Headquarters virus response and reporting activities.

The ASSIST will:

- Coordinate the Headquarters site response to virus/malware incidents by activating an appropriate Virus Response Team (ViRT). If the incident impacts headquarters wide network services, the ASSIST will contact the NSM and other Associate CIO for Operations teams as necessary.
- Provide reports of virus encounters at Headquarters to DOE's Computer Incident Advisory Capability (CIAC).
- Provides training (yearly) to all ViRT members in Headquarters organizations.

Headquarters organizations must have one or more computer support staff or IT-oriented users attend Virus Response Team (ViRT) Training once a year. Headquarters organizations will notify the ASSIST (via their ViRT members) of any virus incident and implement corrective actions identified by CIAC or the ASSIST, and in accordance with established ASSIST procedures (see Virus Response Procedures which are maintained by the ASSIST). Additionally, Headquarters organizations are responsible for identifying variations, if any, in HQ site procedures and policies that are unique to their organization, interoperability clusters, systems, or major applications. This information should be provided in their organizational or major application CSPP.

Special Considerations

- Any automated capabilities for reporting virus encounters must be activated, with the DOE Headquarters ASSIST included in any notification list.
- Features in applications that generate alerts to potential virus situations (such as macro existence alerts) at the desktop computer must be activated. It is not necessary that these features be set to the highest security level, but must be set at least to a level that provides notifications. Other inherent virus protection features in programs and applications must be activated where practical.

- Where applicable, any patches or service packs that address potential virus issues must be applied to applications and operating systems *as soon as practical*.

- If the infection is found on a computer system (and not removable media or an externally received file), the user will not attempt or elect to remove the virus, as some viruses cause damage during removal or require additional corrective actions. A ViRT member must perform complete eradication and recovery. A Virus Investigation Form (see Virus Response Procedures which are maintained by the ASSIST) must be provided by the ViRT member to the DOE Headquarters ASSIST within one working day. The organization will also perform a self-assessment of the failure and institute corrective actions.

- Continual auditing (including, but not restricted to, automated verification from network servers) will be performed to ensure compliance with these policies.

Individuals operating a DOE computer system will not willfully create or transmit malware-infected material to other systems or persons by any means.

5. Contamination By Classified Information Policy

Policy

The Office of the Chief Information Officer (CIO), as the central cyber security authority for the Headquarters site, will utilize the following cyber security policies pertaining to a contamination of the Headquarters network infrastructure by classified information. The Department of Energy (DOE) policy mandates that, once an electronic medium is contaminated with classified data, that medium is deemed classified and must be marked, processed, protected, and destroyed according to the highest level and most restrictive category of the information it contains.

[Note: In many cases, a practical method of recovering from contamination incidents can be implemented without compromising security. This is accomplished by performing *decontamination procedures on* the affected system that allows it to be returned to service in an unclassified mode. Decontamination is not appropriate in all instances. The more stringent DOE policy will be followed when necessary.]

Upon discovery, notification, or even suspicion of contamination by any Headquarters site user, that individual will take action to report the incident and protect the system at the proper (highest) level of classification.

Note: All notes, printouts, or other data resulting from the decontamination procedure will be protected as classified material and handled and disposed of according to the highest level and most restrictive category of the information on the contaminated media. During the incident, all knowledge of a contamination is considered sensitive.

Scope

This policy affects all organizations operating on the Headquarters site network.

Roles and Responsibilities

The Classified Information Systems Operations Manager (ISOM) will act as the coordinator for Headquarters response and reporting activities pertaining to the contamination by classified information.

The Associate CIO for Operations has established the DOE Headquarters Automated Systems Security Incident Support Team (ASSIST) which provide technical assistance, guidance, and review for Headquarters decontamination. The CIO provides 24-hour-a-day, 7-day-a-week cyber security coverage via the Infrastructure Support Center (Help Desk) at 301-903-2500 (response number 2) reporting system. Help Desk staff will notify the ASSIST of any contamination incidents.

If the incident impacts headquarters wide network services, the ASSIST will contact the NSM and other Associate CIO for Operations teams as necessary.

Headquarters organizations are responsible for ensuring that individuals within their organizations are provided with the procedures for dealing with contamination of classified information.

Individuals, upon discovery, notification, or even suspicion that electronic medium is contaminated with classified data will:

- Immediately log off any networks or other shared devices and properly close down and power off the contaminated system. **The User will take no action to attempt to remove or alter the classified data or files, nor take any other steps towards decontamination.**

- Report the incident to the Infrastructure Support Center (Help Desk) at 301-903-2500 (response number 2), the ISOM, or to the HSO for the organization. In any case, the user should state only that a contamination has occurred and provide ONLY name, organization, and telephone number information. Details on the system(s) involved or the data must NOT be provided.

- Protect the system at the proper (highest) level of classification for the classified data currently on it. The user must stay with the contaminated system and protect it from any access until a Security Officer arrives.

- Protect all information relevant to the contamination. The fact that a system is contaminated is considered sensitive information and should not be divulged to anyone without a need to know. No details should be divulged over an unsecured telephone.

- Assist in the decontamination procedure by providing the necessary information in person to the Security Officer. This information includes identifying contaminated files and e-mail messages.